STAT

STAT

STAT

STAT

Page Denied

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

EXECUTIVE STEERING GROUP
for Strategic INFOSEC Planning

Serial: Q1-2106-88
25 July 1988

MEMORANDUM FOR THE MEMBERS, EXECUTIVE STEERING GROUP
MEMBERS, JOINT WORKING GROUP

SUBJECT: Publication of Documents

1. Enclosed for your retention are the final versions of the documents developed by the Joint Working Group and approved by the Executive Steering Group. They include:

a. the Charter, which represents a collective commitment to achieve a successful INFOSEC posture through the combined efforts of both the military and civil sectors of the government;

b. the Terms of Reference, which provides projected milestones for accomplishing the effort; and

c. the Goals and Objectives, representing the heart of the plan, and providing a broad, coherent strategy for INFOSEC government-wide. Specific subobjectives are tied to the development of secure products, mission-specific secure systems, and support services.

2. Through efforts already under way, the Joint Working Group is proceeding with plan development as directed by the steering group.

STAT

[redacted]

Chairman

3 Encls:
a/s

OC-11108X/88

EXECUTIVE STEERING GROUP
for Strategic INFOSEC Planning

CHARTER

for the

Executive Steering Group
and

Joint Working Group

for

Strategic INFOSEC Planning

July 15, 1988

E.

CHARTER
for the
EXECUTIVE STEERING GROUP
and
JOINT WORKING GROUP
for
STRATEGIC INFOSEC PLANNING

1. **AUTHORITY:** The Director, National Security Agency, in his role as the National Manager, NTISS, began a joint planning effort to develop a National Information Systems Security Plan (NISSP). In collaboration with the National Bureau of Standards and their responsibilities under Public Law 100–235, the plan will provide protection strategies for all categories of classified and sensitive information generated, stored, processed, transferred, or communicated by Federal telecommunications and automated information systems. The plan will focus on broad goals and specific objectives which must be attained to achieve an acceptable information systems security posture for the U.S. over a term spanning approximately 10–15 years beyond current initiatives. The National Manager established a Joint Executive Steering Group to direct this effort, and a Joint Working Group to develop the plan.

2. **EXECUTIVE STEERING GROUP:** The Executive Steering Group is chaired by a senior NSA executive, with voluntary representatives from:

Assistant Secretary of Defense (Command, Control, Communications & Intelligence)
Central Intelligence Agency
Commandant, Marine Corps
Defense Investigative Service
Department of the Army
Department of Commerce
Department of Energy
Department of State
Department of Treasury
Federal Bureau of Investigation
General Services Administration
Joint Chiefs of Staff
National Aeronautics and Space Administration

National Bureau of Standards
National Communications System
National Security Agency

The steering group is staffed with senior agency and departmental representatives who have both subject matter expertise and the ability to speak authoritatively for the agencies or departments they represent——the idea is to expedite the development of conclusive solutions to issues and to expedite the process of interagency coordination of the plan. The steering group will provide direction and guidance during development of the plan; is authorized to task the working group, as appropriate; will vote on issues as they surface; and will serve as advisors to the working group. In addition, the steering group will support implementation of the plan, as appropriate, at all levels of the government.

3. **JOINT WORKING GROUP:** The Joint Working Group is co–chaired by NSA and a civil agency. Since NBS has concluded that a shortage of manpower resources precludes them from assuming co–chairmanship at this time, GSA was selected to serve as co–chair for the short–term. NBS is expected to assume the co–chair in the future. Voluntary representatives serving on this group include:

Air Force Cryptologic Support Center
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Central Intelligence Agency
Commandant, U.S. Coast Guard
Commander, Naval Security Group
Defense Investigative Service
Defense Logistics Agency
Department of Agriculture
Department of the Army
Department of Commerce
Department of Energy
Department of State
Department of Transportation
Department of Treasury
Federal Bureau of Investigation
General Services Administration
Headquarters, Electronic Security Command
Headquarters, Intelligence and Security Comand
Headquarters, U.S. Air Force

Headquarters, U.S. Marine Corps
Joint Chiefs of Staff
National Aeronautics and Space Administration
National Bureau of Standards
National Security Agency
Office of Chief of Naval Operations
Stategic Defense Initiative Office

Joint Working Group representatives will volunteer to serve on Working Teams (each with a Team Leader) established by the co–chairmen to address specific areas/issues/objectives of the plan. Team Leaders will brief the Executive Steering Group, as necessary, on the progress of their efforts; and are responsible for the timely completion of their assigned tasks.

4. OPERATING PROCEDURES:

a. Frequency of Meetings:

(1) The Executive Steering Group will meet at least once every three months, or as directed by the Chairman. Alternates may attend for primary members; however, Joint Working Group members will not serve as alternates on the Executive Steering Group.

(2) The Joint Working Group will meet at least once every two months, or as determined by the Co–Chairmen. Alternate members should be designated to provide complete coverage.

(3) Working Teams will meet on an as required basis, to be determined by the Team Leader.

b. **Voting:** Each member of the Executive Steering Group is permitted one vote. Voting decisions will be made by a majority. The Chair will vote in the event of a tie.

c. The Executive Secretary, Joint Working Group will provide the agenda for and summations of both steering and working group meetings, together with the action items which result.

d. Members of both the steering and working groups may propose agenda issues, as the need arises, through their respective Chairmen.

e. All Working Team actions will have the consensus of the Joint Working Group membership before presentation to the Executive Steering Group.

f. The Co–chairs, Joint Working Group, will follow–up on all actions assigned and provide to the Executive Steering Group periodic reports on their status.

g. Prior to commencing plan development, the Joint Working Group will prepare for steering group approval:

(1) Terms of Reference (TOR) that will describe briefly the composition of the plan——i.e., the plan objective, scope, anticipated product, milestones, etc., and

(2) Broad goals and specific objectives which represent those capabilities that the U.S. will require to assure the security and integrity of telecommunications and automated information systems.

5. The Joint Working Group will ensure that the National Information Systems Security Plan is kept current and is responsive to national requirements and priorities by proposing modifications to established tasks and recommending additional tasks when needed.

EXECUTIVE STEERING GROUP
for Strategic INFOSEC Planning

TERMS OF REFERENCE

for the

National Information Systems Security Plan

July 15, 1988

# TERMS OF REFERENCE
for the
NATIONAL INFORMATION SYSTEMS SECURITY PLAN

I. PLAN OBJECTIVE:

The objective of the National Information Systems Security Plan (NISSP) is to focus on broad goals and specific objectives that can be sufficiently linked to the U.S. objectives, and effectively drive future information systems security program actions.

II. SCOPE:

The plan will provide protection strategies for all categories of classified and sensitive information generated, stored, processed, transferred, or communicated by U.S. Government telecommunications and automated information systems.

III. ANTICIPATED PRODUCT:

The National Information Systems Security Plan (NISSP) will focus on broad goals and specific objectives that can be sufficiently linked to the U.S. objectives, and effectively drive future information systems security program actions. Strategies will be provided that address the current and projected environment, and how we expect to approach it in order to achieve the specific objectives. Resource projections to adequately support the objectives will be identified, together with impact statements for not achieving the objectives.

IV. PROJECTED MILESTONES:

15 May 1988	———	Charter Approved by Executive Steering Group
15 May 1988	———	Terms of Reference (TOR) Approved by Executive Steering Group
15 May 1988	———	Goals and Objectives Approved by Executive Steering Group

15 May 1988	Structure/Format Approved by Executive Steering Group
1 Jun 1988	Begin Plan Development
15 Jan 1989	Draft Plan Completed
15 Jan 1989	Begin Plan Coordination Process
15 Jan 1990	Plan Approved by Executive Steering Group
1 Feb 1990	Plan Promulgated by Director, National Bureau of Standards and Director, National Security Agency
15 Feb 1990	Plan Published

V. PLAN COORDINATION:

The Executive Steering Group will ensure extensive coordination throughout the Federal community. The co–chairs of the Joint Working Group are charged to effect such coordination throughout the community of interest as identified by the Executive Steering Group.

VI. IMPLEMENTATION RESPONSIBILITIES:

Implementation of the plan is the responsibility of the heads of departments and agencies of the U.S. Government. The Executive Steering Group will monitor community implementation.

VII. LINKAGES TO OTHER PLANS AND DOCUMENTS:

The plan must be consistent with existing National Policy, Goals, and Objectives; near and mid–term programmatic actions; and current and projected user requirements. Also, the plan must be compatible with other plans within the community. Inputs from the following documents and initiatives were considered and, in most cases. incorporated:

A. Annual Assessment of the Status of Telecommuncations and Automated Information Systems Security Within the United States Government.

B. Director, NSA's Five INFOSEC Thrusts.

C. NSDD 145.

D. NSDD 238.

E. Public Law 100–235 (Computer Security Act of 1987)

F. National INFOSEC Manual.

G. DCI Intelligence Community Automated Information Systems (AIS) and Networks Threat Statement.

H. Final Report of the Industry Information Security (IIS) Task Force titled Industry Information Protection, June 1988.

ENCL. 3

EXECUTIVE STEERING GROUP
for Strategic INFOSEC Planning

GOALS AND OBJECTIVES

for the

National Information Systems Security Plan

July 15, 1988

GOALS AND OBJECTIVES
for the
NATIONAL INFORMATION SYSTEMS SECURITY PLAN

GOAL:

TO ACHIEVE A U.S. INFORMATION SYSTEMS SECURITY PROGRAM THAT PROVIDES FOR THE PROTECTION OF INFORMATION GENERATED, STORED, PROCESSED, TRANSFERRED, OR COMMUNICATED IN TELECOMMUNICATIONS AND/OR AUTOMATED INFORMATION SYSTEMS.

OBJECTIVES:

I. Devise planning, development, and production strategies which will ensure a rich mix of interoperable, user–acceptable security products and systems.

II. Improve the countermeasure techniques available for achieving mission specific information systems security protection ensuring connectivity, survivability and endurability.

III. Achieve a significant improvement in the support services necessary to effectively and efficiently satisfy the users' information systems security needs.

SUBOBJECTIVES:

A. Secure all classified and, where applicable, sensitive telephone communications by significantly increasing the availability of secure telephones.

A. Upgrade national leadership information systems security, including those associated with continuity of government, by integrating appropriate state–of–the–art technologies.

A. Encourage and support research and development in the technology of computer security; and develop guidelines and operational doctrine for trusted computer systems.

SUBOBJECTIVES: (continued)

B. Provide automated key management systems that are secure, user–friendly and interoperable.

C. Encourage the development of embedded secure products, including vendor standard product offerings, in order to provide low–cost, transparent, user–friendly security for telecommunications and automated information systems.

D. Expeditiously secure unprotected radio systems that carry government classified and/or sensitive information.

E. Continue U.S. dominance in developing and marketing cryptology, thus facilitating and promoting interoperability.

F. Develop methodologies to facilitate design, manufacturing, programming, and testing of AISS in a trusted fashion.

G. Speed up the implementation of secure automated information systems which include adequate system security features.

B. Provide necessary mechanisms to secure selected financial information systems and networks, to include all Federal electronic funds transfer systems.

C. Provide protection to improve the utility and survivability of both U.S. and Allied space systems.

D. Develop a comprehensive program to secure data networks and associated office automation equipment.

E. Identify and implement countermeasures needed to offset hazards created by the presence of foreign nationals in sensitive government and industrial areas in the U.S. and abroad, pursuant to provisions of international treaties and other agreements.

B. Improve and expand the methods and technologies needed to assess and disseminate awareness of security risks, threats, vulnerabilities and countermeasure requirements of telecommunications and automated information systems.

C. Develop alternative mechanisms for funding information systems security acquisition initiatives which benefit the Federal Government.

D. Develop procurement mechanisms to significantly improve the acquisition of information system products.

E. Increase information systems security awareness such that it becomes a permanent and necessary feature of Federal operations; establish education and training programs, with meaningful career incentives for the associated professionals.

F. Develop physical security technologies to minimize control and safeguarding requirements, while reducing the vulnerability of systems to the human intelligence (HUMINT) threats.

EXECUTIVE STEERING GROUP
for Strategic INFOSEC Planning

MEMBERSHIP ROSTER

July 15, 1988

EXECUTIVE STEERING GROUP FOR STRATEGIC INFOSEC PLANNING

	Chairman	Dr. William A. Thayer (CHAIR)	301-688-7154
	ASD(C3I)	Ms. D. Diane Fountaine	202-695-7181
STAT	CIA	[redacted]	[redacted]
	CMC	COL W. M. Lazar, USMC	202-694-1197
	DIS	Mr. J. William Leonard	202-475-0931
	DA	COL Albert J. Kondi, USA	202-697-1492
	D/Commerce	Mr. Thomas W. Zetty	202-377-1332
	DOE	Mr. David W. Rowland	301-353-4620
	D/State	Mr. F. Lynn McNulty	202-653-9858
	D/Treasury	Mr. J. Martin Ferris	202-566-2679
	FBI	Mr. William A. Bayse	202-324-5350
	GSA	Mr. Jon P. Stairs	202-426-2100
	JCS	MGen Wayne O. Jefferson, Jr., USAF	202-695-1369
	NASA	Mr. Arthur L. C. Sigust	202-453-2008
	NBS	Dr. Dennis Branstad	301-975-2913
	NCS	COL Charles L. Gordon, USA	202-692-3762
STAT	NSA/S	[redacted]	301-688-6745

NSA/T	[redacted]	301-688-7726
NSA/Q	[redacted] EX/SEC)	301-688-5168

EXECUTIVE STEERING GROUP FOR STRATEGIC INFOSEC PLANNING

STAT

Chairman

[redacted]
Director of Plans
National Security Agency
Fort George G. Meade, MD 20755

301/688-7154

ASD(C3I)

Ms. D. Diane Fountaine
Director, Information Systems
The Pentagon, Room 3E187
Washington, DC 20301

202/695-7181

CIA

(Inside Envelope)

STAT

[redacted]
Deputy Director, Office of Communications

STAT

[redacted]
Central Intelligence Agency
Langley, VA 20505

[redacted]

(Outside Envelope)
Office of Communications
Central Intelligence Agency
Langley, VA 20505

CMC

Colonel W. M. Lazar, USMC
Head, Telecommunications Branch
C4 Systems Division
Headquarters, Marine Corps
Washington, DC 20380

202/694-1197

DIS	Mr. J. William Leonard Chief, Programs Management Division Defense Investigative Service 1900 Half Street, S.W. Washington, DC 20324–1700	202/475–0931
DA	Colonel Albert J. Kondi, USA Chief, Information Systems Security Office Department of the Army The Pentagon, Room 1A474 Washington, DC 20301–0107	202/697–1492
D/Commerce	Mr. Thomas W. Zetty Chief, Telecommunications Management Division Department of Commerce Room 6625 14th and Constitution Avenue, N.W. Washington, DC 20230	202/377–1332
DOE	Mr. David W. Rowland Director of ADP & Telecommunications Planning & Integrity Department of Energy MA–254 GTN Washington, DC 20545	301/353–4620
D/State	Mr. F. Lynn McNulty Department of State DS/ST/ISS Room 2430 N.S. Washington, DC 20520	202/653–9858

D/Treasury

Mr. J. Martin Ferris
Assistant Director, Security Programs
Department of Treasury
Room 2415
1500 Pennsylvania Avenue, N.W.
Washington, DC 20220

202/566-2679

FBI

Mr. William A. Bayse
Assistant Director, Technical Services Division
Federal Bureau of Investigation
Room 7159
10th & Pennsylvania Avenue, N.W.
Washington, DC 20305

202/324-5350

GSA

Mr. Jon P. Stairs
Director, Information Security Management Division
General Services Administration
Room 5680,
7th and D Streets, S.W.
Washington, DC 20407

202/426-2100

JCS

MGen Wayne O. Jefferson, Jr., USAF
Deputy Director for Defense-Wide C3 Support
OJCS
The Pentagon, Room 2D860
Washington, DC 20301

202/695-1369

NASA

Mr. Arthur L. C. Sigust
HQ, National Aeronautics and Space Administration
Code TS
600 Independence Avenue, S.W.
Washington, DC 20546

202/453-2008

	NBS	Dr. Dennis Branstad Technology A-216 National Bureau of Standards Gaithersburg, MD 20899 *(Classified)* National Bureau of Standards Gaithersburg, MD 20899 ATTN: Mrs. Dovey Kaetzel Security Office Admin A-700	301/975-2913
	NCS	Colonel Charles L. Gordon, USA Assistant Deputy Manager National Communications System Washington, DC 20305	202/692-3762
STAT	NSA/S	[redacted] Assistant Deputy Director for Information Security for Business Development National Security Agency Fort George G. Meade, MD 20755-6000	301/688-6745
STAT	NSA (T)	[redacted] Telecommunications and Computer Services Organization National Security Agency Fort George G. Meade, MD 20755-6000	301/688-7726
STAT	Ex/Sec	[redacted] Office of National Plans National Security Agency Fort George G. Meade, MD 20755	301/688-5168